UNITED STATES DISTRICT COURT FOR
THE EASTERN DISTRICT OF PENNSYLVANIA

STEPHEN BASSON 311 Conestoga Way, Apt F68 Eagleville, PA 19403 *Individually and on behalf of all others similarly situated*, Plaintiff, v. **FLORIDA WATER PRODUCTS, LLC**, 7440 State Highway 121, McKinney, TX 75070 Defendant.	CASE NO. 2:24-cv-926 JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Stephen Basson ("Mr. Basson" or "Plaintiff") brings this action on behalf of himself and all others similarly situated, against Defendant, Florida Water Products ("FWP" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

SUMMARY OF THE CASE

1. On May 28, 2023, FWP, a distributor of pool and spa supplies, discovered it had lost control over its computer network and the highly sensitive personal information stored on the computer network in a data breach by cybercriminals ("Data Breach").[1] On information and belief, the Data Breach has impacted thousands of employees.

2. Due to Defendant's intentionally obfuscating language, it is unclear when the Data Breach precisely occurred and how long cybercriminals had unfettered access to Plaintiff's and

[1] California Office of Attorney General, Submitted Breach Notification Sample, https://oag.ca.gov/ecrime/databreach/reports/sb24-577763 (last visited February 28, 2024).

the Class's highly sensitive information. However, on information and belief, the Data Breach occurred on or around May 22, 2023, and was discovered by FWP on May 28, 2023.[2] On or around June 29, 2023, Defendant's investigations revealed that cybercriminals gained unauthorized access to current and former employees' personally identifiable information ("PII").[3]

3. On or about December 8, 2023– almost seven months after the Data Breach occurred– FWP finally notified Plaintiff and Class Members about the Data Breach ("Breach Notice"). A sample of the Breach Notice is attached as Exhibit A.

4. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering them easy targets for cybercriminals.

5. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its employees how many people were impacted, how the breach happened, or why it took the Defendant almost seven months to begin notifying victims that cybercriminals had gained access to their highly private information.

6. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

---

[2] *Id.*
[3] Montana Department of Justice, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-569.pdf (last visited February 28, 2024).

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

8. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its affiliates' current and former employees.

9. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff Stephen Basson is an employee of Aquarius Supply. Aquarius Supply and FWP are both subsidiaries of Heritage Supply Groups. Plaintiff is a Data Breach victim.

11. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

12. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

13. Plaintiff, Stephen Basson, is a natural person and citizen of Pennsylvania, residing in Eagleville, Pennsylvania, where he intends to remain.

14. Defendant Florida Water Products, LLC is a Florida Limited Liability Company with its principal place of business at 7440 State Highway 121, McKinney, TX 75070.

JURISDICTION & VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Plaintiff and Defendant are citizens of different states.

16. This Court has personal jurisdiction over Defendant because Defendant does substantial business in this District and employs people who reside in this District.

17. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

FACTUAL ALLEGATIONS

Florida Water Products

18. FWP is a wholesale distributor of pool and spa equipment. According to its website, FWP's vision is to "serve [their] employees, customers, and suppliers not only through pool supply distribution but as a life betterment company." FWP attributes its 35 years of steady growth to "the concept of treating employees and customers as valued partners."[4]

19. On information and belief, FWP was acquired by the Heritage Pool Supply Group in December 2021.[5] Both Heritage Pool Supply Group and its sister company, Heritage Landscape

[4] FWP, About, https://fwppool.com/about/ (last visited February 28, 2024).
[5] Pool and Spa News, https://www.poolspanews.com/business/heritage-pool-supply-acquires-florida-water-products-bel-aqua-hachik-and-others-to-accelerate-national-plan_o (last visited February 28, 2024).

Supply Group, are wholly owned subsidiaries of SRS Distribution Inc. Heritage Landscape Group acquired Aquarius Supply in October 2020.[6]

20. On information and belief, FWP accumulates highly sensitive PII of its employees.

21. On information and belief, FWP maintains the PII in its computer systems, including a legacy data repository.

22. In collecting and maintaining employees' PII, Defendant agreed it would safeguard data in accordance with state law and federal law. After all, Plaintiff and class members took reasonable steps to secure their PII.

23. Despite recognizing its duty to do so, on information and belief, FWP has not implemented reasonably cybersecurity safeguards or policies to protect employees' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, FWP leaves significant vulnerabilities in its own systems for cybercriminals to exploit and gain access to employees' PII.

FWP Fails to Safeguard Employees' PII

24. Plaintiff has been an employee of Aquarius Supply for fourteen years. Aquarius was acquired by Heritage (FWP's parent company) in October 2020.[7]

25. As a condition of employment with Aquarius Supply, Plaintiff was required to provide his PII, including at least his name and Social Security Number.

26. In collecting and maintaining PII, FWP implicitly agrees it will safeguard the data using reasonable means according to its internal policies and state and federal law.

---

[6] Heritage Landscape Supply Group, Aquarius Supply has joined the Heritage Family of Companies, https://www.heritagelandscapesupplygroup.com/en/news/#ThirteenthNews (last visited February 28, 2024).

[7] *Id.*

27. According to the December 8, 2023 Breach Notice, FWP experienced a security incident "that temporarily impacted the availability and functionality of a legacy data repository" in which "an unauthorized actor may have accessed and acquired certain files contained within this legacy environment." Ex. A.

28. "Legacy data" is "information that is stored in outdated or obsolete systems, formats or technologies."[8] Legacy data is more vulnerable to security threats because it is typically stored in outdated systems that were designed without modern security threats in mind.[9]

29. Due to Defendant's incredibly obfuscating information, the precise dates on which the Data breach occurred and how long cybercriminals had access to Plaintiff's and the Class's most sensitive information is currently unknown. However, on information and belief, the breach took place between May 22, 2023 and May 28, 2023.[10]

30. Defendant's internal investigation that did not conclude until September 21, 2023, an appalling four months after Defendant discovered its Breach, revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing thousands of FWP and its affiliates' employees' personal, private, and sensitive information, including but not limited to employees' names and Social Security numbers. Ex. A.

31. In other words, the Data Breach investigation revealed Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of individuals' highly private information.

---

[8] Cloudficient, What is Legacy Data?, https://www.cloudficient.com/blog/what-is-legacy-data (last visited February 28, 2024).

[9] Synchrony Systems, Inc., 5 Ways Your Legacy Systems May Add to Cybersecurity Risks, https://sync-sys.com/5-ways-your-legacy-systems-may-add-to-cybersecurity-risks/ (last visited February 28, 2024).

[10] California Office of Attorney General, Submitted Breach Notification Sample, https://oag.ca.gov/ecrime/databreach/reports/sb24-577763 (last visited February 28, 2024).

32. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiff would not have accepted Defendant's or its affiliates' employment offer, nor provided his PII, had he known that FWP and its affiliates does not take all necessary precautions to secure the personal data given to it by employees.

33. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

34. On or about August 17, 2023– almost three months after the Data Breach occurred– FWP finally began notifying individuals about the Data Breach. However, Plaintiff was not notified until December 8, 2023, almost seven months after the data breach occurred.

35. Despite its duties and alleged commitments to safeguard PII, FWP does not follow industry standard practices in securing employees' PII, as evidenced by the Data Breach and stolen employee PII.

36. In response to the Data Breach, FWP contends that it has "decommissioned the legacy environment, and we are continuing to train our employees concerning data security." Ex. A. Although Defendant fails to expand on what the alleged training consists of, such training should have been in place prior to the Data Breach. Additionally, Defendant's legacy system should have been decommissioned before the Data Breach.

37. Through its Breach Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to read "more information on identity theft protection" and it provided "additional steps you can take in response to this incident." Ex. A.

38. FWP further acknowledges through its Breach Notice, its duty to implement reasonable cybersecurity safeguards or policies to protect its employees PII, promising that, despite the Data Breach demonstrating otherwise, it "recognizes the importance of protecting the personal information it maintains" and "take[s] the privacy and confidentiality of information in [its] care very seriously…" Ex. A.

39. On information and belief, FWP has offered only twelve months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

40. Even with one year of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, FWP failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

43. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

44. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[11]

45. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), FWP knew or should have known that its electronic records would be targeted by cybercriminals.

46. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

47. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

48. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

49. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of its

---

[11] CNET, Data breaches break record in 2021, https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited February 28, 2024).

employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII.

50. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

51. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its employees' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience and Injuries

52. Plaintiff has been an employee of Aquarius Supply for fourteen years. Aquarius Supply and FWP are both subsidiaries of Heritage Supply Groups.

53. As a condition of employment with Aquarius Supply, Plaintiff was required to provide his PII.

54. Plaintiff provided his PII and trusted that FWP and its affiliates would use reasonable measures to protect it according to Defendants internal policies, as well as state and federal law.

55. Defendant sent Plaintiff his Breach Notice on December 8, 2023, depriving Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects for almost seven months.

56. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

57. Plaintiff suffered actual injury from the exposure of his PII —which violates his rights to privacy.

58. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

59. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and monitoring his credit information.

60. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

61. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's egregious seven-month delay in informing Plaintiff and Class Members about the Data Breach.

62. Indeed, following the Data Breach, Plaintiff has experienced an enormous increase in spam texts daily, suggesting that his PII is in the hands of cybercriminals.

63. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

64. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

65. As a result of FWP failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession

66. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

67. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

68. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

69. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

70. One such example of criminals using PII for profit is the development of "Fullz" packages.

71. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

72. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII

stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

73. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

74. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

75. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

76. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

77. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

78. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee, data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

81. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

82. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

83. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

84. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

85. Plaintiff is suing on behalf of himself and the proposed Class ("Class"), defined as follows:

> **All individuals whose PII was compromised in the Florida Water Products Data Breach, including all those who received notice of the breach.**

86. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

87. Plaintiff reserves the right to amend the class definition.

88. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes at least thousands of individuals who have been damaged by Defendant's conduct as alleged herein.

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel

experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

89. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

90. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

91. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

92. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass.

93. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

94. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and

occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

95. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's personal information and PII.

96. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of employee PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII.

97. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

98. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have

suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

99. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

100. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

101. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

102. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

103. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as

described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

104. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

105. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

106. Defendant breached its duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

107. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

108. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and the Class would not have been injured.

109. The injury and harm suffered by Plaintiff and the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

110. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including but not limited to loss of time researching the data breach;

loss of time monitoring credit information; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

111. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

112. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

113. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

114. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

115. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

116. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

117. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Class)

118. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

119. At all times during Plaintiff' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' personal data that Plaintiff and Class Members provided to Defendant.

120. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' personal data would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

121. Plaintiff and Class Members provided their respective personal data to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the personal data to be disseminated to any unauthorized parties.

122. Plaintiff and Class Members also provided their respective personal data to Defendant with the explicit and implicit understanding that Defendant would take precautions to

protect that personal data from unauthorized disclosure, such as following basic principles of information security practices.

123. Defendant voluntarily received in confidence Plaintiff's and Class Members' personal data with the understanding that the personal data would not be disclosed or disseminated to the public or any unauthorized third parties.

124. Due to Defendant's failure to prevent, detect, and/or avoid the data breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' personal data, Plaintiff's and Class Members' personal data was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

125. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

126. But for Defendant's disclosure of Plaintiff's and Class Members' personal data in violation of the parties' understanding of confidence, their personal data would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data breach was thedirect and legal cause of the theft of Plaintiff's and Class Members' personal data, as well as the resulting damages.

127. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' personal data. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' personal data had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

128. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

129. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

130. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

131. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

132. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and by retaining the benefit of Plaintiff's and the Class's labor.

133. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

135. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

136. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

137. Plaintiff and Class Members have no adequate remedy at law.

138. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

139. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

140. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: March 4, 2024

Respectfully submitted,

SALTZ MONGELUZZI & BENDESKY P.C.

By: <u>*/s/ Patrick Howard*</u>
Patrick Howard (PA Atty ID #88572)
1650 Market St., 52 Fl.
Pennsylvania, PA 19103
(215) 496-8282
phoward@smbb.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Raina C. Borrelli (*Pro Hac Vice* forthcoming)
Samuel J. Strauss (*Pro Hac Vice* forthcoming)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com